



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/916,395	07/27/2001	Tomomi Haruna	16869S-030000US	7769

20350 7590 01/17/2006

TOWNSEND AND TOWNSEND AND CREW, LLP  
TWO EMBARCADERO CENTER  
EIGHTH FLOOR  
SAN FRANCISCO, CA 94111-3834

EXAMINER

MILIA, MARK R

ART UNIT PAPER NUMBER

2622

DATE MAILED: 01/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/916,395

Applicant(s)

HARUNA ET AL.

Examiner

Mark R. Millia

Art Unit

2622

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 30 September 2005.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-6, 8-14, 16-19 and 37-48 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-6, 8-14, 16-19 and 37-48 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

***Response to Amendment***

1. Applicant's amendment was received on 9/30/05 and has been entered and made of record. Currently, claims 1-6, 8-14, 16-19, and 37-48 are pending.

***Priority***

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

***Drawings***

3. Applicant's amendment to the specification to include reference characters "202" and "206" has overcome the objection to Fig. 2 as cited in the previous Office Action. Therefore the objection has been withdrawn.

### ***Claim Objections***

4. Applicant's amendment to make claim 3 dependent from claim 2 has overcome the objection as cited in the previous Office Action. Therefore the objection has been withdrawn.

### ***Response to Arguments***

5. Applicant's arguments filed 9/30/05 have been fully considered but they are not persuasive.

In response to applicant's arguments regarding the rejection of claims 1-6, 8-14, 16-19, and 37-48, more specifically independent claims 1, 4, 12, 14, 116, 17, 37, 41, and 45, wherein on page 15, the applicant asserts that the reference of Alur does not disclose a print terminal located in a user's home and the certificate issuer system being located at a remote location away from the user's home. The examiner respectfully disagrees as the reference of Alur does disclose such features. Particularly, as seen in Fig. 1, column 1 lines 29-43, and column 3 line 48-column 4 line 34 of Alur, it is suggested that the user is located at home. The user interacts with a browser located on a personal computer (client) to input information and request a license (certificate). The client interacts with the host (certificate issuer system) via a network, such as the Internet, and obtains the license that is then printed by printer "107". Therefore, as clearly illustrated in Fig. 1, the print terminal is located in a user's home and the

certificate issuer system is located at a remote location. Further, it is obvious that Fig. 1 of the application is similar to Fig. 1 of Alur. Also, as shown in Fig. 2 of Alur, the verification of a license that has been obtained from host "116" and printed is executed by the authenticator with the aid of the host (certificate issuer system). This is accomplished at a location that is not the user's home. This is analogous to the verification system shown in Fig. 5 of the application, which is also not located at a user's home. Thus, the reference of Alur discloses analogous certificate issuing and certificate verifying systems.

6. Therefore, the rejection of claims 1-6, 8-14, 16-19, and 37-48, as cited in the previous Office Action, is maintained and repeated in this Office Action.

### ***Claim Rejections - 35 USC § 103***

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1-6, 8-14, 16-19, and 37-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alur in view of Want.

Regarding claim 1, Alur discloses in a certificate issuing system comprising: a print terminal having print means for printing certificate data on a print form (see Fig. 1 (107)), input means for inputting personal certification ID (see Fig. 1 (104)), and print terminal communication means (see Fig. 1, column 3 line 66-column 4 line 3, and column 4 lines 20-34), and a certificate issuer system (host 116) having certificate

issuer communication means for performing communication with said print terminal (see Fig. 1 (114) and (118)), certificate storage means for storing said certificate data (see Fig. 1 (124)), and issue management storage means for storing certificate issue management data (see Fig. 1 (122)), a certificate issuing method comprising the steps of: sending said personal certification ID to said certificate issuer system from said print terminal through said print terminal communication means, wherein said print terminal is located in a user's home and said certificate issuer system is located at a remote location away from said user's home (see Fig. 1, column 1 lines 29-43, and column 3 line 48-column 4 line 34, and column 5 lines 10-65), reading said certificate data in association with said personal certification ID from said certificate storage means of said certificate issuer system (see Fig. 1, column 4 lines 12-18, and column 5 lines 13-35), storing said certificate data to be issued in association with said issue management storage means of said certificate issuer system after personal certification ID is received at said certificate issuer system through said certificate issuer communication means (see Fig. 1 (124), column 4 lines 15-18, and column 5 lines 53-65), sending said read certificate data indicating that said certificate data to be printed on said print form is verified through said certificate issuer communication means to said print terminal (see Fig. 1, column 4 lines 28-35, and column 5 lines 61-65, reference shows that the host validates the license using the information provided by the user which is analogous to verifying the certificate data), and printing said certificate data on said print form, after said certificate data is received at said print terminal through said print terminal communication means (see column 4 lines 28-35 and column 5 lines 61-65).

Alur does not disclose expressly a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form.

Want discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 2, Alur discloses in certificate verifying system comprising a verification terminal (see Fig. 2, column 4 lines 40-60, and column 6 line 45-column 7 line 3), display means for displaying received data (see Fig. 2 (204) and column 6 lines 58-60), and verification terminal communication means (see Fig. 2), and a certificate issuer system having certificate issuer communication means for performing communication with said verification terminal (see Figs. 1 and 2 and column 4 lines 51-60, reference shows that host (116) must be in communication with the verification terminal (204) because it utilizes permutation maps (122), also a portable computer (204) is capable of connecting to network (114) for access to host (116) as is well known in the art), certificate storage means for storing said certificate data (Fig. 1 (124)) and issue management storage means for storing certificate issue management data (Fig. 1 (122)), a certificate verifying method comprising the steps of: sending an identification number to said certificate issuer system from said verification terminal through said verification terminal communication means, after an identification number is read by said verification terminal (see column 4 lines 40-60 and column 6 line 45-

column 7 line 3), reading said certificate data in association with said received ID number at said certificate issuer system with reference to said issue management storage means and said certificate storage means, and sending said certificate data to said verification terminal through said certificate issuer communication means (see Fig. 2 and column 6 line 45-column 7 line 3), and displaying said certificate data on said display means, after said certificate data is received through said verification terminal communication means, wherein said certificate data is obtained at a user's home (Fig. 1, column 1 lines 29-43, column 3 line 48-column 4 line 34, and see column 6 lines 58-60).

Alur does not disclose expressly a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form.

Want discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 4, Alur discloses in a certificate issuer system comprising: certificate issuer communication means for performing communication with a print terminal (see Fig. 1), certificate storage means for storing certificate data (see Fig. 1 (124)), and issue management storage means for storing certificate issue management data (see Fig. 1 (122)), said certificate issuer system being capable of performing communication with said print terminal having print means for printing said certificate



data on a print form, input means for inputting personal certification ID (see Fig. 1 (104)), and print terminal communication means (see Fig. 1, column 3 line 66-column 4 line 3, and column 4 lines 20-34), a certificate issuing method comprising the steps of: receiving said personal certification ID through said certificate issuer communication means, after said personal certification ID is sent from said print terminal (see Fig. 1, column 3 line 66-column 4 line 3, column 4 lines 6-34, and column 5 lines 10-65), reading said certificate data in association with said personal certification ID from said certificate storage means (see Fig. 1, column 4 lines 12-18, and column 5 lines 13-35), storing said received ID number and said certificate data to be issued in association with said issue management storage means (see Fig. 1 (124) and column 4 lines 15-18), sending said certificate data in association with said certificate ID, as data to be printed on said print form, to said print terminal through said certificate issuer communication means (see Fig. 1, column 4 lines 28-35, and column 5 lines 61-65), and wherein said print terminal is located in a user's home and said certificate issuer system is located at a remote location away from said user's home (see Fig. 1, column 1 lines 29-43, and column 3 line 48-column 4 line 34), and wherein when said print terminal is to print out said received certificate data, said print terminal reads said ID number again, verifies whether said ID number read again is identical with said ID number sent already to said certificate issuer or not, and prints said certificate data on said print form after said verification is made (see column 5 lines 10-65).

Alur does not disclose expressly a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form.

Want discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 12, Alur discloses in a certificate issuer system comprising: a certificate issuer system located at a remote location away from a user's home having certificate issuer communication means for performing communication with a verification terminal (see Figs. 1 and 2, column 3 line 48-column 4 line 34, and column 4 lines 51-60, reference shows that host (116) must be in communication with the verification terminal (204) because it utilizes permutation maps (122), also a portable computer (204) is capable of connecting to network (114) for access to host (116) as is well known in the art), certificate storage means for storing certificate data (Fig. 1 (124)), and issue management storage means for storing certificate issue management data (Fig. 1 (122)), said certificate issuer system being capable of performing communication with said verification terminal having ID number reading means (see Figs. 1 and 2 (204) and (206)), display means for displaying received data (see Fig. 2 (204) and column 6 lines 58-60), and verification terminal communication means (see Fig. 2), a certificate verifying method comprising the steps of: receiving ID number through said certificate issuer communication means, after said ID number is sent from said verification

terminal (see Figs. 1 and 2, reference shows that the ID number is verified by the use of the database and permutation maps located in the host (116) which is analogous to the certificate issuer of the claim limitation), reading said certificate data in association with said received ID number with reference to said issue management storage means and said certificate storage means (see Fig. 2, reference shows that the ID number is verified by the use of the database and permutation maps located in the host (116)), and sending said read certificate data to said verification terminal through said certificate issuer communication means so that said certificate data is displayed to indicate that when said print form is attached with said ID, said form is verified on said display means of said verification terminal (see Fig. 2 and column 6 lines 58-60, reference shows that an authenticator verifies the license by comparing the information gathered from the portable computer, which interacts with the license database and inherently has a display, with the information contained in the license, all of which is analogous to the claim limitation).

Alur does not disclose expressly a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form.

Want discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 14, Alur discloses a certificate issuing system comprising: certificate issuer communication means performing communication with a print terminal located in a user's home having print means for printing certificate data on a print form (see Fig. 1, column 4 lines 15-35, and column 5 lines 10-65), input means for inputting personal certification ID (Fig. 1 (104)), and print terminal communication means (see Fig. 1), certificate storage means for storing said certificate data (see Fig. 1 (124)), issue management storage means for storing certificate issue management data (see Fig. 1 (122)), and control means for controlling said certificate issuer communication means, said certificate storage means and said issue management storage means (see Fig. 1 (118)), wherein, when said personal certification ID sent from said print terminal are received through said certificate issuer communication means (see column 4 lines 20-35), said control means performs control so as to read said certificate data in association with said personal certification ID from said certificate storage means, so as to store said received ID number and said certificate data to be issued in association with said issue management storage means, and so as to send said certificate data in association with said personal certification ID, as data to be printed on said print form, to said print terminal through said certificate issuer communication means (see column 5 lines 10-65), wherein said certificate issuer communication means is capable of performing communication with a verification terminal having ID reading means for reading an ID attached to a print form on which certificate data is printed, display means for displaying received data, and verification terminal communication means (see Fig. 2, column 4 lines 36-59, and column 6 line 41-column 7 line 3), and wherein, when said ID

sent from said verification terminal is received through said certificate issuer communication means, said control means performs control so as to read said certificate data in association with said received ID from said issue management storage means and said certificate storage means, and controls said certification issuer communication means to send said read certificate data to said verification terminal so that said certificate data is displayed to indicate that when said print form is attached with said ID said form is verified on said display means of said verification terminal (see Fig. 2, column 4 lines 36-59, and column 6 line 41-column 7 line 3, reference shows that an authenticator verifies the license by comparing the information gathered from the portable computer, which interacts with the license database and inherently has a display, with the information contained in the license, all of which is analogous to the claim limitation).

Alur does not disclose expressly a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form.

Want discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 16, Alur discloses a certificate verifier system comprising: certificate verifier communication means performing communication with a verification terminal located at a remote location away from a print terminal located in a user's

Art Unit: 2622

home reading means for reading ID numbers (see Fig. 2, column 4 lines 40-60, and column 6 line 45-column 7 lines 3), display means for displaying received data (see Fig. 2 (204) and column 6 lines 58-60), and verification terminal communication means (see Fig. 2), certificate storage means for storing said certificate data (Fig. 1 (124)), issue management storage means for storing certificate issue management data (Fig. 1 (122)), and control means for controlling said certificate verifier communication means, said certificate storage means and said issue management storage means (see Fig. 2 (202) and (204)), wherein, when ID number sent from said verification terminal is received through said certificate verifier communication means, said control means performs control so as to read said certificate data in association with said received ID number from said issue management storage means and said certificate storage means, and controls said certificate verifier communication means to send said read certificate data to said verification terminal so that said certificate data is displayed to indicate that when said print form is attached with said ID, said form is verified on said display means of said verification terminal (see Figs. 1 and 2, column 4 lines 40-60, and column 6 line 45-column 7 line 3, reference shows that an authenticator verifies the license by comparing the information gathered from the portable computer, which interacts with the license database and inherently has a display, with the information contained in the license, all of which is analogous to the claim limitation).

Alur does not disclose expressly a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form.

Art Unit: 2622

Want discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 17, Alur discloses a certificate issuing machine comprising: a database for storing personal ID and identity papers, which are provided by an applicant, in association with personal data of said applicant (see Fig. 1 (124) and column 4 lines 15-18), a communication interface for receiving a request made by said applicant for applying for a certificate to which a personal identification number is attached, and for receiving data in association with an ID number attached to said certificate made by said request for applying for said certificate (see Fig. 1, column 4 lines 15-35, and column 5 lines 10-65), and a controller connected to said database and said communication interface so as to perform control such that said personal data in said database in association with said personal identification number and said identity papers is sent to said applicant for issuing said certificate which is to be verified when said ID is attached to said certificate through said communication interface in a form of said requested certificate, wherein said certificate issuing machine is located at a remote location away from a print terminal located in a user's home (see Fig. 1 (118), column 4 lines 28-35, and column 6 line 41-column 7 line 3).

Alur does not disclose expressly a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form.

Art Unit: 2622

Want discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claims 37, 41, and 45, Alur discloses a system of printing in a printer terminal which communicates with a data manager comprising: sending an ID number to the data manager (see 4 lines 20-35), receiving data for printing sent from the data manager (see Fig. 1 and column 4 lines 28-35), and printing the data for printing onto the paper so that said paper is verified, wherein at least some of the data for printing are associated with the ID number in the data manager, wherein said print terminal is located in a user's home (see Fig. 1, column 4 lines 28-35 and column 5 lines 61-65, reference shows that the host validates the license using the information provided by the user which is analogous to verifying the certificate data).

Alur does not disclose expressly reading a microchip ID of a microchip attached to a paper.

Want discloses reading a microchip ID of a microchip attached to a paper (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Alur & Want are combinable because they are from the same field of endeavor, use of identification numbers to execute desired procedures.

At the time of the invention, it would have been obvious to a person of ordinary skill in the art to combine the electronic tag (microchip) attached to a print form,



Art Unit: 2622

containing an identification number, that provides various digital services in response to the presentation of the identification number of the electronic tag as described by Want with the system of Alur as an additional identification number that can be easily verified.

The suggestion/motivation for doing so would have been to provide various digital services, such as that of obtaining a license, by use of an identification number that is easily verified and stored in the memory of the microchip as well as an associated database. Materials containing microchips with embedded identification numbers used to execute some sort of procedure or application are commonly used in the art, i.e. smart cards, and the use of a database to store information regarding a certificate or the like, which is in turn used to verify such information, is also well known and commonly used in the art. Therefore it would have been obvious to use the electronic tag and associated identification number as described by Want as additional input information and ultimately verification information, stored in a database, with the system of obtaining a license via a network as described by Alur.

Therefore, it would have been obvious to combine Want with Alur to obtain the invention as specified in claims 1, 2, 4, 12, 14, 16, 17, 37, 41, and 45.

Regarding claim 3, Alur and Want disclose the system discussed in claim 2, and Alur further discloses wherein said certificate issuer communication means is capable of performing communication with a verification terminal ID number reading means for reading an ID number attached to a print form on which certificate data is printed (see Figs. 1 and 2 and column 6 line 45-column 7 line 3), display means for displaying

received data (see column 6 lines 58-60), and verification terminal communication means (see Fig. 2), and wherein said certificate verifying method comprising the steps of: sending ID number to said certificate issuer system from said verification terminal through said verification terminal communication means, after said ID number is read by said reading means of said verification terminal (see column 4 lines 51-60 and column 6 line 45-column 7 line 3, reference shows that host (116) must be in communication with the verification terminal (204) because it utilizes permutation maps (122), also a portable computer (204) is capable of connecting to network (114) for access to host (116) as is well known in the art), reading said certificate data in association with said received ID number at said certificate issuer system with reference to said issue management storage means and said certificate storage means, and sending said certificate data to said verification terminal through said certificate issuer communication means (see column 6 line 45-column 7 line 3), and displaying said certificate data on said display means of said verification terminal, after said certificate data is received through said verification terminal communication means (see column 6 lines 58-60). Want further discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 5, Alur and Want disclose the system discussed in claim 4, and Alur further discloses wherein said certificate issuer communication means is capable of performing communication with a verification terminal having reading means for reading

an ID number attached to a print form on which certificate data is printed (see Figs. 1 and 2 and column 6 line 45-column 7 line 3), display means for displaying received data (see column 6 lines 58-60), and verification terminal communication means (see Fig. 2), and wherein said certificate issuing method further comprising the steps of: receiving said ID number through said certificate issuer communication means, after said ID number is sent from said verification terminal (see column 4 lines 51-60 and column 6 line 45-column 7 line 3, reference shows that host (116) must be in communication with the verification terminal (204) because it utilizes permutation maps (122), also a portable computer (204) is capable of connecting to network (114) for access to host (116) as is well known in the art), reading said certificate data in association with said ID number received from said issue management storage means and said certificate storage means (see column 6 line 45-column 7 line 3), and sending said read certificate data to said verification terminal through said certificate issuer communication means so that said certificate data is displayed on said display means of said verification terminal (see column 6 line 45-column 7 line 3). Want further discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 6, Alur and Want disclose the system discussed in claim 4, and Alur further discloses wherein a personal identification number, as well as said personal certification ID, is sent from said print terminal (see column 4 lines 20-27 and column 5 lines 17-25). Want further discloses a microchip attached to a print form and microchip

reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 8, Alur and Want disclose the system discussed in claim 4, and Alur further discloses wherein said personal certification ID is ID which is issued when an applicant for applying for a certificate registers said certificate data in said certificate issuer and which is stored in association with said certificate data (see column 4 lines 28-35).

Regarding claim 9, Alur and Want disclose the system discussed in claim 4, and Alur further discloses wherein said certificate issuer system further comprises a fee charging means, said fee charging means charging a fee when said certificate data is issued (see column 4 lines 9-11 and column 5 lines 40-42).

Regarding claim 10, Alur and Want disclose the system discussed in claim 5, and Alur further discloses sending a mail address, as well as said personal certification ID, from said print terminal (see column 4 lines 25-26), storing said sent mail address in said issue management storage means (see column 4 lines 15-18), and sending a notification that there is a verification request to said mail address stored in said issue management storage means, when said request for verification is made from said verification terminal (see column 6 line 45-column 7 line 3, reference shows that the user is notified of the result of the verification process, it is well known in the art to use various methods of notifying a user of such a process, one of which being notification via a mail address, therefore it would have been obvious to use such a method of

Art Unit: 2622

notification as claimed). Want further discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 11 Alur and Want disclose the system discussed in claim 5, and Alur further discloses wherein, when a request for applying for one kind of certificate, as well as said personal certification ID, is sent from said print terminal, said certificate issuer system sends certificate data corresponding to said sent request (see column 4 lines 20-35 and column 5 lines 10-65). Want further discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claim 13, Alur and Want disclose the system discussed in claim 12, and Alur further discloses storing a mail address together with said certificate data in said certificate storage means (see column 4 lines 15-18), and sending a notification that there is a verification request to said stored mail address, when said request for verification is made from said verification terminal (see column 6 line 45-column 7 line 3, reference shows that the user is notified of the result of the verification process, it is well known in the art to use various methods of notifying a user of such a process, one of which being notification via a mail address, therefore it would have been obvious to use such a method of notification as claimed).

Regarding claim 18, Alur and Want disclose the system discussed in claim 17, and Alur further discloses a charging unit for storing a fee in accordance with transmission of said personal data of said database in said certificate form correspondingly to said personal data of said applicant in said database, in conformity with a condition of said certificate issuing request (see Fig. 1 (120), column 4 lines 9-11, and column 5 lines 40-55).

Regarding claim 19, Alur and Want disclose the system discussed in claim 18, and Alur further discloses wherein data for requesting said corresponding fee stored in said database is sent to said communication interface in association with a verification request for verifying said issued personal data of said applicant (see column 5 lines 40-55).

Regarding claims 38, 42, and 46, Alur and Want disclose the system discussed in claims 37, 41, and 45, and Alur further discloses reading the ID number again (see column 5 lines 10-65), before printing verifying whether the ID number read again is identical with the ID number sent to the data manager (see column 5 lines 10-65). Want further discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claims 39, 43, and 47, Alur and Want disclose the system discussed in claims 37, 41, and 45, and Alur further discloses sending a request for applying one type of printing data with the ID number to the data manager (see column 4 lines 20-35

and column 5 lines 10-65). Want further discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

Regarding claims 40, 44, and 48, Alur and Want disclose the system discussed in claims 37, 41, and 45, and Alur further discloses sending a personal certificate ID and a personal identification number to the data manager (see column 4 lines 20-27 and column 5 lines 17-25). Want further discloses a microchip attached to a print form and microchip reading means for reading microchip ID in a microchip attached to a print form (see Figs. 1 and 5 (20), column 6 lines 36-48 and 53-58, column 8 line 66-column 9 line 6, and column 11 lines 41-43).

### ***Conclusion***

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

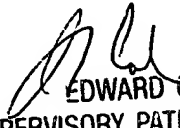
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mark R. Milia whose telephone number is (571) 272-7408. The examiner can normally be reached M-F 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edward Coles can be reached at (571) 272-7402. The fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mark R. Milia  
Examiner  
Art Unit 2622

MRM

  
EDWARD COLES  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 26